UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/709,398	05/02/2004	Ihab Shraim	040246-000100US	3397

20350 7590 09/02/2009

TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER	
TESLOVICH, TAMARA	
ART UNIT	**PAPER NUMBER**
2437	

MAIL DATE	DELIVERY MODE
09/02/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/709,398	SHRAIM ET AL.	
	Examiner	Art Unit	
	Tamara Teslovich	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 April 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-40,43-50 and 53-74* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-40,43-50 and 53-74* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *04.30.08, 08.13.08, 08.15.08, 09.15.08, 10.22.08, 02.27.09, 03.30.09,* .
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This Office Action is in response to Applicant's Remarks and Amendments filed April 30, 2009.

Claims 1, 4, 5, 9, 15-17, 25, 36-40, 43, 53 and 61-64 are amended.

Claims 41, 42, 51 and 52 are cancelled.

Claim 74 is new.

Claims 1-40, 43-50 and 53-74 are pending and herein considered.

Response to Arguments

Applicant's arguments filed April 30, 2009 have been fully considered but they are not persuasive.

Applicant's amendments to claim 36 serve to overcome the Examiner's 35 USC 101 rejections of claims 36-42 as being directed to nonstatutory subject matter. Accordingly, those rejections have been withdrawn.

The Examiner respectfully disagrees with Applicant's arguments concerning the Golan provisional and its alleged failure to teach or suggest that which is taught by the Golan PCT, including those portions cited by the Examiner as teaching the elements of the pending claims. Specificity regarding particular portions of the Golan provisional serving to anticipate Applicant's claims is provided below.

The Examiner respectfully disagrees with Applicant's next set of arguments concerning the cited references' failure to teach or suggest "wherein the instructions executable to investigate the uniform resource locator comprise instructions to:

download at least one web page from the server references by the uniform resource locator, and analyze the at least one web page to determine whether the at least one web page comprises a data collection mechanism for allowing a user to provide personal information to the server references by the at least one uniform resource locator" as claimed in claim 12 and similarly claimed in claim 1. Applicant's arguments fail entirely to account for the Examiner's rejection of claim 12 and the subject matter therein in view of Oliver. While the Examiner does not concede that Shipp fails entirely to mention the use of forms or other data collection mechanisms, she has withdrawn her rejection of the claims in view of Shipp for the time being in order to further prosecution by limiting the number of references under discussion at once. Unfortunately for Applicant, those claims rejected in view of Shipp remain rejected in view of Oliver and insofar as Applicant has failed entirety to respond to those rejections, the Examiner has no choice but to maintain them.

The Examiner respectfully disagrees with Applicant's next set of arguments concerning Oliver's failure to teach or suggest instructions executable to "obtain information about an address the uniform resource locator purports to reference but actually does not reference" and "compare the ascertained address with the information about the address the uniform resource locator purports to reference" as claimed in claim 9. The Examiner would like to draw attention to paragraph 13 of Oliver wherein he teaches the examination of "reference points" such as URL links, email addresses with well known domain names, and any other contact or identity information associated with a well known entity. Oliver goes on to discuss how this "information" may be

compared in order to determine the legitimacy of the message. Oliver even goes so far as to provide for those situations where the legitimacy remains at question even after such a comparison. In paragraph 14 Oliver specifically provides for the use of the references address in the comparison. It is based upon these portions of the reference in view of the reference in its entirety that the Examiner maintains her position that Oliver does in fact anticipate Applicant's instructions executable to obtain information about an address the uniform resource locator purports to reference but actually does not reference and compare the ascertained address with the information about the address the uniform resource locator purports to reference.

The Examiner respectfully disagrees with Applicant's next set of arguments concerning Golan's failure to teach or suggest "downloading a web page from a suspicious server," "parsing the web page to identify at least one field in which a user may enter personal information," and "analyzing the at least one field to identify a type of information requested by the at least one field" as taught in claim 18. The Examiner would like to begin by calling attention to page 7 of the provisional wherein Golan discusses pre-processing in order to determine whether a particular email or communication is legitimate. While Golan provides a number of alternate ways to make that determination throughout his reference, his use of clogging in particular for websites that attempt to collect data from customers particularly anticipates Applicant's downloading of a web page from a suspicious server, parsing that page to identify at least one field, and analyzing that information so that his system may create a database of false information with which to fill the rogue forms in order to not only dilute the

information collected by the suspicious form but also to place in the hands of the phishers information which may be used to track them down.

It is in view of the portions cited above in view of the references in their entirety that they Examiner maintains her rejection of the claims in their entirety. Those rejections have been provided below in a form to reflect Applicant's amendments. Any claims not particularly mentioned above remain rejected as presented below.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-17 and 74 are rejected under 35 U.S.C. 102(e) as being anticipated by United States Patent Application Publication 2007/0101423 A1 to Oliver et al.

As per **claim 1**, Oliver teaches in a relationship between a fraud protection provider and a customer, a system for combating online fraud, the system comprising: a monitoring center for monitoring a suspicious email activity, the monitoring center comprising (par 12): a first computer, the first computer comprising instructions executable by the first computer to allow an analysis of an investigation of a uniform

resource locator (pars 12-13); a first telecommunication link configured to provide communication between a technician and the customer, such that the technician can notify the customer of a result of the investigation of a uniform resource locator and the customer can provide instructions for responding to a fraudulent attempt to collect personal information (par 19); and a second telecommunication link configured to provide data communication between the monitoring center and at least one additional computer (par 12); and a second computer in communication with the monitoring center via the second telecommunication link, the second computer including instructions executable by the second computer to: gather an incoming email message, the incoming email message comprising a uniform resource locator (pars 12-13); analyze the incoming email message (pars 12-13); based on an analysis of the incoming email message, categorize the incoming email message as a possibly fraudulent email message (pars 17-18); and investigate the uniform resource locator included in the incoming email message to determine whether a location referenced by the incoming email message is associated with a fraudulent attempt to collect personal information (par 13); and wherein the instructions executable to investigate the uniform resource locator comprise instructions to download at least one web page from the server referenced by the uniform resource locator, and analyze the at least one web page to determine whether the at least one web page comprises a data collection mechanism for allowing a user to provide personal information to the server referenced by the at least one uniform resource locator (pars 26-27).

As per **claim 2**, Oliver teaches a system for combating online fraud as recited in claim 1, wherein the first computer comprises further instructions executable by the first computer to analyze an investigation of a uniform resource locator (pars 14, 20-24).

As per **claim 3**, Oliver teaches a system for combating online fraud as recited in claim 1, wherein the first computer comprises further instructions executable by the first computer to allow a technician to analyze an investigation of a uniform resource locator (pars 15, 19).

As per **claim 4**, Oliver teaches in a relationship between a fraud protection provider and a customer, a computer system for combating online fraud, the computer system comprising: a processor (par 12); and a computer readable medium in communication with the processor, the computer readable medium comprising instructions executable by the processor to (pars 12-13): gather an incoming email message, the incoming email message comprising a uniform resource locator (pars 12-13); analyze the incoming email message (pars 12-13); based on an analysis of the incoming email message, categorize the incoming email message as a possibly fraudulent email message (pars 17-18); investigate the uniform resource locator included in the incoming email message to determine whether a location referenced by the incoming email message is associated with a fraudulent attempt to collect personal information (par 13); and initiate a response to the fraudulent attempt to collect personal information (par 16); and wherein investigating the uniform resource locator comprises

downloading at least one web page from the server referenced by the uniform resource locator, and analyzing the at least one web page to determine whether the at least one web page comprises a data collection mechanism for allowing a user to provide personal information to the server referenced by the at least one uniform resource locator (pars 26-27).

As per **claim 5**, Oliver teaches a computer system for analyzing a suspicious email message, the computer system comprising: a processor (pars 12-13); and a computer readable medium in communication with the processor, the computer readable medium comprising instructions executable by the processor to (pars 12-13): parse the suspicious email message to identify a header portion of the suspicious email message, a body portion of the suspicious email message, and a uniform resource locator portion of the suspicious email message (par 17); analyze the header portion of the suspicious email message (par 17); analyze the body portion of the suspicious email message (par 17); analyze the uniform resource locator portion of the suspicious email message (pars 17, 20-24); and categorize the suspicious email message as a possibly fraudulent email message (pars 18-19); and wherein the instructions executable to investigate the uniform resource locator comprise instructions to download at least one web page from the server referenced by the uniform resource locator and analyze the at least one web page to determine whether the at least one web page comprises a data collection mechanism for allowing a user to provide personal information to the server referenced by the at least one uniform resource locator (pars 26-27).

As per **claim 6**, Oliver teaches a computer system for analyzing a suspicious email message as recited in claim 5, wherein the instructions are further executable by the processor to: based on the analysis of the header portion of the email message, assign a score to the header portion of the suspicious email message and compare the score assigned to the header portion of the suspicious email message with a threshold score for the header portion of the suspicious email message (pars 17-20); based on the analysis of the body portion of the suspicious email message, assign a score to the body portion of the suspicious email message and compare the score assigned to the body portion of the suspicious email message with a threshold score for the body portion of the suspicious email message (pars 17-20); and based on the analysis of the uniform resource locator portion of the suspicious email message, assign a score to the uniform resource locator portion of the suspicious email message (pars 17-20).

As per **claim 7**, Oliver teaches a computer system for analyzing a suspicious email message as recited in claim 6, wherein the computer readable medium comprises further instructions executable by the processor to: compare the score assigned to the uniform resource locator portion of the suspicious email message with a threshold score for the uniform resource locator portion of the suspicious email message (pars 17-20); and based on the comparison of the score assigned to the uniform resource locator portion of the suspicious email message and the threshold score for the uniform

resource locator portion of the suspicious email message, categorize the suspicious email message as a possibly fraudulent email message (pars 17-20).

As per **claim 8**, Oliver teaches a computer system for analyzing a suspicious email message as recited in claim 6, wherein the computer readable medium comprises further instructions executable by the processor to: compute a composite score based on the score assigned to the header portion of the suspicious email message, the score assigned to the body portion of the suspicious email message and the score assigned to the uniform resource locator portion of the suspicious email message (pars 17-20); assign the composite score to the suspicious email message; compare the composite score assigned to the suspicious email message with a threshold composite score for the suspicious email message and based on the comparison of the composite score assigned the suspicious email message and the threshold score for the suspicious email message, categorize the suspicious email message as a possibly fraudulent email message (pars 17-20).

As per **claim 9**, Oliver teaches a computer system for investigating a suspicious uniform resource locator to determine whether a server referenced by the uniform resource locator may be involved in fraudulent activity, the computer system comprising: a processor (pars 12-13); and a computer readable medium in communication with the processor, the computer readable medium comprising instructions executable by the processor to (pars 12-13): ascertain an address

associated with a server referenced by the uniform resource locator (pars 21, 24, 25); obtain information about an address the uniform resource locator purports to reference but actually does not reference (pars 14-15); compare the ascertained address associated with the information about the address the uniform resource locator purports to reference (pars 14-15); and based on the comparison of the ascertained address and the information about the address the uniform resource locator purports to reference, determine whether the uniform resource locator is fraudulent (par 16).

As per **claim 10**, Oliver teaches a computer system for investigating a suspicious uniform resource locator as recited in claim 9, wherein computer readable medium comprises further instructions executable to interrogate the server referenced by the uniform resource locator (par 25).

As per **claim 11**, Oliver teaches a computer system for investigating a suspicious uniform resource locator as recited in claim 9, wherein computer readable medium comprises further instructions executable to generate an event report (pars 12, 19, 28).

As per **claim 12**, Oliver teaches a computer system for investigating a suspicious uniform resource locator as recited in claim 10, wherein interrogating the server referenced by the uniform resource locator comprises: downloading at least one web page from the server referenced by the uniform resource locator; and analyzing the at least one web page to determine whether the at least one web page comprises a field

for allowing a user to provider personal information to the server referenced by the at least one uniform resource locator (pars 26-27).

As per **claim 13**, Oliver teaches a computer system for investigating a suspicious uniform resource locator as recited in claim 10, wherein interrogating the server referenced by the uniform resource locator comprises: examining the server for vulnerabilities that indicate the server possible has been compromised (pars 21-25).

As per **claim 14**, Oliver teaches a computer system for investigating a suspicious uniform resource locator as recited in claim 9, wherein ascertaining an address associated with the server referenced by the uniform locator comprises tracing a route to the server referenced by the uniform resource locator (pars 20, 22, 24, 25).

As per **claim 15**, Oliver teaches a computer system for investigating a suspicious uniform resource locator as recited in claim 9, wherein obtaining information about an address the uniform resource locator purports to reference comprises parsing an anchor associated with the uniform resource locator to identify an apparent address for a server referenced by the uniform resource locator (pars 21-25)

As per **claim 16**, Oliver teaches a computer system for investigating a suspicious uniform resource locator as recited in claim 15, wherein obtaining information about an address the uniform resource locator purports to reference further comprises obtaining

WHOIS information about the apparent address for the server referenced by the uniform resource locator (par 15).

As per **claim 17**, Oliver teaches a computer system for investigating a suspicious uniform resource locator as recited in claim 9, wherein obtaining information about an address the uniform resource locator purports to reference comprises parsing an anchor associated with the uniform resource locator to identify a trusted entity apparently referenced by the uniform resource locator (pars 21-25).

As per **claim 74**, Oliver teaches a system for combating online fraud as recited in claim 1, wherein the web page comprises a form and the data collection mechanism comprises one or more fields on the form (pars 26-27).

Claims 18-40, 43-50, 53-60 and 62-63 are rejected under 35 U.S.C. 102(e) as being anticipated by United States Patent Application Publication 2008/0052359 A1 to Golan et al.

As per **claim 18**, Golan teaches a computer system for responding to a fraudulent attempt to collect personal information, the computer system comprising: a processor (pars 27, 30); and a computer readable medium in communication with the processor, the computer readable medium comprising instructions executable by the processor to (pars 27, 30): download a web page from a suspicious server and parse

the web page to identify at least one field into which a user may enter personal information (pars 31-32); analyze the at least one field to identify a type of information requested by the at least one field (pars 31-32); generate a set of safe data comprising personal information associated with a fictitious entity (pars 31-32); based on an analysis of the at least one field, select at least a portion of the set of safe data comprising the type of information requested by the at least one field (pars 31-33); format a response to the web page, the response including the portion of the safe data comprising the type of information requested by the at least one field (pars 31-33); and transmit the response to the web page for reception by the suspicious server (pars 31-33).

As per **claim 19**, Golan teaches a computer system for responding to a fraudulent attempt to collect personal information as recited in claim 18, wherein analyzing the at least one field to identify a type of information requested by the field comprises interpreting a label associated with the at least one field (par 43).

As per **claim 20**, Golan teaches a computer system for responding to a fraudulent attempt to collect personal information as recited in claim 18, wherein the set of safe data is associated with a financial account, and wherein the computer readable medium comprises further instructions executable by the processor to: monitor the financial account for an account activity evidencing a use of information obtained from

the set of safe data; and trace the account activity to identify an entity using the information obtained from the set of safe data (pars 32, 37).

As per **claim 21**, Golan teaches a computer system for responding to a fraudulent attempt to collect personal information as recited in claim 18, wherein the computer readable medium comprises further instructions executable by the processor to: generate a plurality of sets of safe data, each of the sets of safe data comprising personal information associated with a fictitious entity (par 44); based on an analysis of the at least one field, select at least a portion of each of the sets of safe data responsive to the at least one field (pars 43-44); format a plurality of responses to the web page, each of the plurality of response including the portion of one of the sets of safe data, each of the portions of one of the sets of safe data being responsive to the at least one field (pars 43-44; 46); and transmit the plurality of responses to the web page for reception by the suspicious server (pars 43-44; 46).

As per **claim 22**, Golan teaches a computer system for responding to a fraudulent attempt to collect personal information as recited in claim 21, wherein the computer readable medium comprises further instructions executable by the processor to: transmit for reception by the suspicious server a number of responses to the web page sufficient to cause a recipient of the responses to be uncertain which of a plurality of responses include valid personal information (pars 33, 36).

As per **claim 23**, Golan teaches a computer system for responding to a fraudulent attempt to collect personal information as recited in claim 21, wherein the computer readable medium comprises further instructions executable by the processor to: transmit for reception by the suspicious server a number of responses to the web page sufficient to indicate that the fraudulent attempt to collect personal information has been discovered (pars 33, 36, 41).

As per **claim 24**, Golan teaches a computer system for responding to a fraudulent attempt to collect personal information as recited in claim 21, wherein the computer readable medium comprises further instructions executable by the processor to: transmit for reception by the suspicious server a number of responses to the web page sufficient to prevent the suspicious server from receiving any responses comprising valid personal information (pars 33, 36, 41).

As per **claim 25**, Golan teaches in a relationship between a fraud protection provider and a customer, a system for combating online fraud, the system comprising: a monitoring center for monitoring a suspicious email activity, the monitoring center comprising a first computer, the first computer including instructions executable by the first computer to allow the analysis of the suspicious email activity and the initiation of a response to the suspicious email activity (pars 27, 28); a second computer in communication with the monitoring center, the second computer including instructions executable by the second computer to gather an incoming email message addressed to

at least one bait email address that has been seeded at a location on a computer network likely to be a target for a third party attempting to harvest email addresses, the incoming email message including a uniform resource locator configured to direct a recipient of the incoming email message to a web site referenced by the uniform resource locator (pars 30, 31); and a third computer in communication with the second computer and further in communication with the monitoring center, the third computer including instructions executable by the third computer to: analyze the incoming email message (par 32); based on an analysis of the incoming email message, categorize the incoming email message as a fraudulent email message (par 32); investigate the uniform resource locator included with the incoming email message to determine information about a server hosting the web site referenced by the uniform resource locator (par 32); and prepare a report comprising at least some of the information about the server hosting the web site referenced by the uniform resource locator (par 28); wherein the instructions executable to investigate the uniform resource locator comprise instructions to download at least one web page from the server referenced by the uniform resource locator, and analyze the at least one web page to determine whether the at least one web page comprises a data collection mechanism for allowing a user to provide personal information to the server referenced by the at least one uniform resource locator (pars 3, 5, 31, 32, 44, 45).

As per **claim 26**, Golan teaches a system for combating online fraud as recited in claim 25, wherein the first computer includes further instructions executable by the first

computer to notify the customer that a fraudulent email message has been received (par 19).

As per **claim 27**, Golan teaches a system for combating online fraud as recited in claim 25, wherein the first computer includes further instructions executable by the first computer to analyze the suspicious email activity (pars 28, 32).

As per **claim 28**, Golan teaches a system for combating online fraud as recited in claim 25, wherein the first computer includes further instructions executable by the first computer to allow a technician to analyze the suspicious email activity (pars 9, 18, 19, 30).

As per **claim 29**, Golan teaches a system for combating online fraud as recited in claim 25, wherein the first computer and the second computer are the same computer (pars 27, 30, 31).

As per **claim 30**, Golan teaches a system for combating online fraud as recited in claim 25, wherein the second computer and the third computer are the same computer (pars 27, 30, 31).

As per **claim 31**, Golan teaches a system for combating online fraud as recited in claim 25, wherein the first computer includes further instructions executable by the first

computer to allow a technician to initiate an administrative response against an operator of the server (pars 9, 18, 19, 30).

As per **claim 32**, Golan teaches a system for combating online fraud as recited in claim 25, wherein the first computer includes further instructions executable by the first computer to pursue an administrative response against an operator of the server (pars 9, 18, 19, 30).

As per **claim 33**, Golan teaches a system for combating online fraud as recited in claim 25, wherein the first computer includes further instructions executable by the first computer to allow a technician to initiate a technical response against an operator of the server hosting the web site referenced by the uniform resource locator (pars 9, 18, 19, 30, 33, 36, 41).

As per **claim 34**, Golan teaches a system for combating online fraud as recited in claim 33, the system further comprising a set of at least one computer, each computer of the set of at least one computer including instructions executable by that computer to pursue a technical response against the server (pars 9, 18, 19, 30, 33, 36, 41).

As per **claim 35**, Golan teaches a system for combating online fraud as recited in claim 34, wherein the set of at least one computer comprises a plurality of computers,

such that pursuing a technical response against the server comprises pursuing a distributed technical response against the server (pars 9, 18, 19, 30, 33, 36, 41).

As per **claim 36**, Golan teaches a computer readable medium comprising a software application including instructions that are executable by a computer to: create at least one safe account, the at least one safe account being associated with at least one bait email address (pars 32, 44); seed the at least one bait email address at a location on a computer network, the location being a likely target for a third party attempting to harvest email addresses (pars 25, 32, 44); gather an incoming email message addressed to the at least one bait email address, the incoming email message including a uniform resource locator configured to direct a recipient of the incoming email message to a web site referenced by the uniform resource locator (pars 30, 31); analyze the incoming email message (par 32); based on an analysis of the incoming email message, categorize the incoming email message as a possibly fraudulent email message (par 32); investigate the uniform resource locator included with the incoming email message to determine information about a server hosting the web site referenced by the uniform resource locator (par 32); prepare a report comprising at least some of the information about the server hosting the web site referenced by the uniform resource locator (par 28); and allow an analysis of the report to determine whether the server is likely to attempt to fraudulently collect personal information (pars 25, 28, 32); wherein the instructions executable to investigate the uniform resource locator comprise instructions to download at least one web page from the server referenced by the

uniform resource locator, and analyze the at least one web page to determine whether the at least one web page comprises a data collection mechanism for allowing a user to provide personal information to the server referenced by the at least one uniform resource locator (pars 3, 5, 31, 32, 44, 45).

As per claim **37**, Golan teaches a computer readable medium as recited in claim 36, wherein the computer software application is further executable by a computer to analyze the report to determine whether the server is likely to attempt to fraudulently collect personal information (pars 6, 26, 28).

As per **claim 38**, Golan teaches a computer readable medium as recited in claim 36, wherein the computer software application is further executable by a computer to allow a technician to initiate an action in response to a fraudulent attempt by the server to collect personal information (pars 9, 18, 19, 30, 33, 36, 41).

As per **claim 39**, Golan teaches a computer readable medium as recited in claim 36, wherein the computer software application is further executable by a computer to pursue an action in response to a fraudulent attempt by the server to collect personal information (pars 9, 18, 19, 30, 33, 36, 41).

As per **claim 40**, Golan teaches a computer readable medium as recited in claim 36, wherein the computer software application comprises a plurality of interoperable

software modules, such that each of the plurality of interoperable software modules is executable by a different computer (pars 27, 28, 30, 31, 32).

As per **claim 43**, Golan teaches in a relationship between a fraud protection provider and a customer, a method of combating online fraud, the method comprising: creating at least one safe account, the at least one safe account being associated with at least one bait email address (pars 32, 44); seeding the at least one bait email address at a location on a computer network, the location being a likely target for a third party attempting to harvest email addresses (pars 25, 32, 44); gathering an incoming email message addressed to the at least one bait email address, the incoming email message including a uniform resource locator configured to direct a recipient of the incoming email message to a web site referenced by the uniform resource locator (pars 30, 31); analyzing the incoming email message; based on an analysis of the incoming email message, categorizing the incoming email message as a fraudulent email message (par 32); investigating the uniform resource locator included with the incoming email message to determine information about a server hosting the web site referenced by the uniform resource locator (par 32); preparing a report comprising at least some of the information about the server hosting the web site referenced by the uniform resource locator (par 28); analyzing the report to determine whether the server is engaged in a fraudulent attempt to collect personal information (pars 25, 28, 32); and taking an action to respond to the fraudulent attempt to collect personal information (pars 9, 18, 19, 30, 33, 36, 41); wherein investigating the uniform resource locator

comprises downloading at least one web page from the server referenced by the uniform resource locator, and analyzing the at least one web page to determine whether the at least one web page comprises a data collection mechanism for allowing a user to provide personal information to the server referenced by the at least one uniform resource locator (pars 3, 5, 31, 32, 44, 45).

As per **claim 44**, Golan teaches a method of combating online fraud as recited in claim 43, wherein the bait email address is seeded at a location selected from the group consisting of a domain registration record, a newsgroup, an electronic mailing list, an electronic customer list, an online chat room, an online message board and a list of active email addresses (pars 25, 44, 46).

As per **claim 45**, Golan teaches a method of combating online fraud as recited in claim 43, wherein the incoming email message purports to be from the customer (par 37).

As per **claim 46**, Golan teaches a method of combating online fraud as recited in claim 45, wherein the method further comprises establishing a customer profile for the customer, wherein the customer profile includes instructions governing how an attempted online fraud should be handled, and wherein taking an action to respond the fraudulent collection of personal information comprises consulting the customer profile

to determine which of a plurality of actions to take to respond to the fraudulent collection of personal information by the server (pars 19, 24, 32).

As per **claim 47**, Golan teaches a method of combating online fraud as recited in claim 45, wherein taking an action to respond to the fraudulent collection of personal information by the server comprises notifying the customer of the fraudulent attempt to collect personal information (par 19, 32).

As per **claim 48**, Golan teaches a method of combating online fraud as recited in claim 43, wherein taking an action to respond to a fraudulent attempt by the server to collect personal information comprises pursuing an administrative response against an operator of the server (pars 9, 18, 19, 30, 33, 36, 41).

As per **claim 49**, Golan teaches a method of combating online fraud as recited in claim 48, wherein pursuing an administrative response against an operator of the server comprises notifying an Internet service provider associated with the server that the server is engaged in a fraudulent activity (pars 9, 18, 19, 30, 33, 36, 41).

As per **claim 50**, Golan teaches a method of combating online fraud as recited in claim 43, wherein the information about the server indicates that the server has been used compromised in a fraudulent attempt to collect personal information, and wherein taking an action to respond to a fraudulent attempt by the server to collect personal

information comprises notifying an operator of the server that the server has been compromised (pars 9, 18, 19, 30, 33, 36, 41).

As per **claim 53**, Golan teaches a method of combating online fraud as recited in claim 51, wherein taking an action to respond to a fraudulent attempt by the server to collect personal information comprises pursuing a technical response against the server (pars 9, 18, 19, 30, 33, 36, 41).

As per **claim 54**, Golan teaches a method of combating online fraud as recited in claim 53, wherein pursuing a technical response against the server comprises providing fictitious personal information to the server, and wherein the fictitious personal information is formatted to be responsive to the at least one field for providing personal information to a web page hosted by the server (pars 43-44; 46).

As per **claim 55**, Golan teaches a method of combating online fraud as recited in claim 54, wherein the fictitious personal information provided to the server comprises a traceable identifier, and wherein pursuing a technical response against the server comprises tracing a use of the traceable identifier (par 35).

As per **claim 56**, Golan teaches a method of combating online fraud as recited in claim 55, wherein the traceable identifier comprises an account identifier for a financial account associated with the customer (pars 35, 44, 45).

As per **claim 57**, Golan teaches a method of combating online fraud as recited in claim 54, wherein pursuing a technical response against the server comprises providing sufficient fictitious personal information to impede the use of any valid personal information received by the server (pars 9, 18, 19, 30, 33, 36, 41).

As per **claim 58**, Golan teaches a method of combating online fraud as recited in claim 54, wherein pursuing a technical response against the server comprises providing sufficient fictitious personal information to notify an operator of the server that the attempt to fraudulently collect personal information has been discovered (pars 33, 36, 41).

As per **claim 59**, Golan teaches a method of combating online fraud as recited in claim 54, wherein pursuing a technical response against the server comprises providing fictitious personal information at a rate sufficient to impede the server's ability to receive personal information from any other sources (pars 33, 36, 41).

As per **claim 60**, Golan teaches a method of combating online fraud as recited in claim 54, wherein pursuing a technical response against the server comprises transmitting the fictitious personal information from a plurality of computers (pars 38, 39, 40).

As per **claim 62**, Golan teaches a method of combating online fraud as recited in claim 43, wherein investigating the uniform resource locator further comprises ascertaining an Internet Protocol address referenced by the uniform resource locator (par 32).

As per **claim 63**, Golan teaches a method of combating online fraud as recited in claim 43, wherein investigating the uniform resource locator further comprises interrogating the server hosting the web site referenced by the uniform resource locator (par 32).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 61 and 64-73 are rejected under 35 U.S.C. 103(a) as being unpatentable over United States Patent Application Publication 2008/0052359 A1 to Golan et al as applied to claims 43-60 above, and further in view of United States Patent Application Publication 2007/0101423 A1 to Oliver et al.

As per **claim 61**, Golan teaches a method of combating online fraud as recited in claim 43 but fails to specifically teach wherein investigating the uniform resource locator fruther comprises accessing a set of WHOIS information about an apparent address referenced by the uniform resource locator.

Oliver teaches wherein investigating a uniform resource locator included with an incoming email message to determine information about a server hosting the web site referenced by the uniform resource locator comprises accessing a set of WHOIS information about an apparent address referenced by the uniform resource locator (par 15).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to include within Golan's system the capability to access a set of WHOIS information about an address referenced by the uniform resource locator in order to determine whether or not the URL was valid.

As per **claim 64**, Golan teaches a method of combating online fraud as recited in claim 43 but fails to specifically teach wherein investigating the uniform resource locator further comprises tracing a network route to the server.

Oliver teaches a computer system for investigating a suspicious uniform resource locator as recited in claim 9, wherein ascertaining an address associated with the server referenced by the uniform locator comprises tracing a route to the server referenced by the uniform resource locator (pars 20, 22, 24, 25).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to include within Golan's system the capability to trade a route to the server referenced by the URL in order to determine whether or not the URL was valid.

As per **claim 65**, Golan teaches a method of combating online fraud as recited in claim 43 but fails to specifically teach wherein analyzing the incoming email message comprises analyzing a header portion of the incoming email message.

Oliver teaches wherein analyzing the incoming email message comprises analyzing a header portion of the incoming email message (pars 17, 20-24).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to include within Golan's system the capability to analyze a header portion of the incoming email in order to better determine whether or not the email is legitimate.

As per **claim 66**, the combined method of Golan and Oliver teaches a method of combating online fraud as recited in claim 65, wherein analyzing a header portion of the incoming email message comprises determining whether the incoming message is a spoofed message (Oliver pars 18-19).

As per **claim 67**, the combined method of Golan and Oliver teaches a method of combating online fraud as recited in claim 65, wherein analyzing a header portion of the

incoming email message comprises determining whether the incoming email message originates from a suspicious Internet domain (Oliver pars 14-15).

As per **claim 68**, Golan teaches a method of combating online fraud as recited in claim 43 but fails to particularly teach wherein analyzing the incoming email message comprises analyzing a body portion of the incoming email message.

Oliver teaches wherein analyzing the incoming email message comprises analyzing a body portion of the incoming email message (pars 17, 20-24).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to include within Golan's system the capability to analyze a body portion of the incoming email in order to better determine whether or not the email is legitimate.

As per **claim 69**, the combined method of Golan and Oliver teaches a method of combating online fraud as recited in claim 68, wherein analyzing a body portion of the incoming message comprises searching the body portion of the incoming message for strings indicating that the incoming message may be part of an attempt to fraudulently collect personal information (Oliver pars 13, 17).

As per **claim 70**, Golan teaches a method of combating online fraud as recited in claim 43, but fails to specifically teach wherein analyzing the incoming email message

comprises analyzing a uniform resource locator included in the incoming email message.

Oliver teaches analyzing the incoming email message comprises analyzing a uniform resource locator included in the incoming email message (pars 13, 17).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to include within Golan's system the capability to analyze a URL included in the incoming email in order to better determine whether or not the email is legitimate or whether it is an attempt at phishing.

As per **claim 71**, the combined method of Golan and Oliver teaches a method of combating online fraud as recited in claim 70, wherein analyzing a uniform resource locator included in the incoming email message comprises determining whether the uniform resource locator references a suspicious Internet location (Oliver pars 14-15).

As per **claim 72**, Golan teaches a method of combating online fraud as recited in claim 43 but fails to specifically teach wherein analyzing the incoming email message comprises assigning a score to the incoming email message.

Oliver teaches wherein analyzing the incoming email message comprises assigning a score to the incoming email message (pars 17-20).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to include within Golan's system the capability to assign scores to

incoming email messages in order to determine whether or not they are a threat and need to be examined further.

As per **claim 73**, the combined method of Golan and Oliver teaches a method of combating online fraud as recited in claim 72, wherein analyzing the incoming email message further comprises comparing the assigned score with a threshold score (Oliver pars 17-20).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tamara Teslovich whose telephone number is (571)272-4241. The examiner can normally be reached on Mon-Fri 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Tamara Teslovich/
Examiner, Art Unit 2437

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2437